1.	Record Nr.	UNINA9910483399403321
	Titolo	Progress in Cryptology - INDOCRYPT 2008 : 9th International Conference on Cryptology in India, Kharagpur, India, December 14-17, 2008. Proceedings / / edited by Dipanwita Roy Chowdhury, Vincent Rijmen, Abhijit Das
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2008
	ISBN	3-540-89754-2
	Edizione	[1st ed. 2008.]
	Descrizione fisica	1 online resource (XV, 437 p.)
	Collana	Security and Cryptology, , 2946-1863 ; ; 5365
	Classificazione	DAT 465f SS 4800
	Disciplina	005.8
	Soggetti	Cryptography Data encryption (Computer science) Algorithms Computer science - Mathematics Discrete mathematics Data protection Computer networks Electronic data processing - Management Cryptology Discrete Mathematics in Computer Science Data and Information Security Computer Communication Networks IT Operations
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Bibliographic Level Mode of Issuance: Monograph
	Nota di bibliografia	Includes bibliographical references and index.
	Nota di contenuto	Stream Ciphers -- Slid Pairs in Salsa20 and Trivium -- New Directions in Cryptanalysis of Self-Synchronizing Stream Ciphers -- Analysis of RC4 and Proposal of Additional Layers for Better Security Margin -- New Results on the Key Scheduling Algorithm of RC4 -- Cryptographic Hash Functions -- Two Attacks on RadioGatún -- Faster Multicollisions -- A New Type of 2-Block Collisions in MD5 -- New Collision Attacks

against Up to 24-Step SHA-2 -- Public-Key Cryptography – I -- Secure Hierarchical Identity Based Encryption Scheme in the Standard Model -- A Fuzzy ID-Based Encryption Efficient When Error Rate Is Low -- Type-Based Proxy Re-encryption and Its Construction -- Toward a Generic Construction of Universally Convertible Undeniable Signatures from Pairing-Based Signatures -- Security Protocols -- Concrete Security for Entity Recognition: The Jane Doe Protocol -- Efficient and Strongly Secure Password-Based Server Aided Key Exchange (Extended Abstract) -- Round Efficient Unconditionally Secure Multiparty Computation Protocol -- A New Anonymous Password-Based Authenticated Key Exchange Protocol -- Group Key Management: From a Non-hierarchical to a Hierarchical Structure -- Hardware Attacks -- Scan Based Side Channel Attacks on Stream Ciphers and Their Counter-Measures -- Floating Fault Analysis of Trivium -- Algebraic Methods in Side-Channel Collision Attacks and Practical Collision Detection -- Block Ciphers -- New Related-Key Boomerang Attacks on AES -- New Impossible Differential Attacks on AES -- Reflection Cryptanalysis of Some Ciphers -- A Differential-Linear Attack on 12-Round Serpent -- New AES Software Speed Records -- Public-Key Cryptography – II -- A New Class of Weak Encryption Exponents in RSA -- Two New Efficient CCA-Secure Online Ciphers: MHCBC and MCBC -- Cryptographic Hardware.-Chai-Tea, Cryptographic Hardware Implementations of xTEA -- High Speed Compact Elliptic Curve Cryptoprocessor for FPGA Platforms -- Elliptic Curve Cryptography -- More Discriminants with the Brezing-Weng Method -- Another Approach to Pairing Computation in Edwards Coordinates -- Threshold Cryptography -- A Verifiable Secret Sharing Scheme Based on the Chinese Remainder Theorem -- Secure Threshold Multi Authority Attribute Based Encryption without a Central Authority.

Sommario/riassunto

This book constitutes the refereed proceedings of the 9th International Conference on Cryptology in India, INDOCRYPT 2008, held in Kharagpur, India, in December 2008. The 33 revised full papers were carefully reviewed and selected from 111 submissions. The papers are organized in topical sections on stream ciphers, cryptographic hash functions, public-key cryptography, security protocols, hardware attacks, block ciphers, cryptographic hardware, elliptic curve cryptography, and threshold cryptography.